WEBINAR: MINIMIERUNG DER RISIKEN BEI PRIVILEGIERTE BENUTZERKONTEN

first frame networkers

HERZLICH WILLKOMMEN

first frame networkers

Vielen Dank, dass Sie sich die Zeit für uns nehmen!

- **Was Sie heute erwartet:**
  - Ein spannendes Referat über die Minimierung der Risiken bei privilegierte Benutzerkonten.
  - Informationen über den sorgenfreien Betrieb einer PAM-Lösung.
  - Die Möglichkeit unseren Experten Fragen über die Chatfunktion zu stellen.

JÖRG KOCH
Leiter Marketing
first frame networkers ag

UNSERE REFERENTEN

first frame networkers

STEFAN RABBEN

Regional Sales Director DACH
FUDO Security

- Seit Juni 2024 bei FUDO Security.
- Seine Aufgabe: Verkaufsverantwortung für die DACH-Region.
- Diplom-Ingenieur für Informationstechnik, Netzwerk und Medientechnik (Universität Stuttgart).
- In seiner Freizeit steigt er gerne aufs Rennrad oder auf Berge und das am liebsten in Italien.

UNSERE REFERENTEN

first frame networkers

DANILO GIACOMINI

Senior System Engineer & Projektleiter
first frame networkers ag

- Seit einem Jahr bei der first frame networkers ag.
- Seine Aufgabe: Projektleiter mit Schwerpunkt Security.
- Der eidg. dipl. Wirtschaftsinformatiker HF macht derzeit ein Studium zum BSc. in Cyber Security.
- In seiner Freizeit geniesst er das Tauchen in der Schweiz.

AGENDA

first frame networkers

- 11:00 Begrüssung / Jörg Koch
- 11:05 Minimierung der Risiken durch privilegierte Benutzerkonten / Stefan Rabben, FUDO Security
- 11:30 Sorgenfreier Betrieb durch Managed PAM-Service / Danilo Giacomini, first frame networkers ag
- 11:35 Fragen & Antworten
- 11:45 Schluss

first frame networkers

FUDO SECURITY

Einem Sicherheitsvorfall geht immer die Zugriffsverletzung durch ein privilegiertes Konto voraus.

Grundlagen zu PAM

FUDO SECURITY

IDENTITÄTEN
- Menschen, Maschinen -

SICHERE INTERAKTION

ASSETS
- Daten, Anwendungen, Systeme -

Administratoren — **HOHE** Privilegien

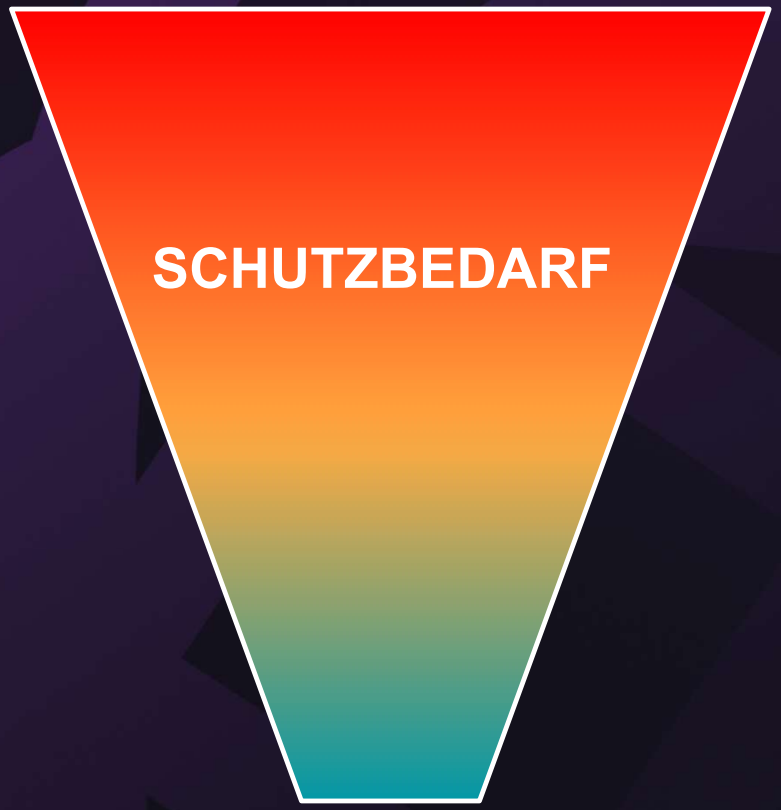
Betriebssysteme	●	Lesen	●
Netzwerk	●	Modifizieren	●
Applikationen	●	Erstellen	●
Dienste	●	Löschen	●

Super User — **MITTLERE** Privilegien

Betriebssysteme		Lesen	●
Netzwerk		Modifizieren	●
Applikationen	●	Erstellen	
Dienste		Löschen	

Standard User — **NIEDRIGE** Privilegien

Betriebssysteme		Lesen	●
Netzwerk		Modifizieren	
Applikationen	●	Erstellen	
Dienste		Löschen	



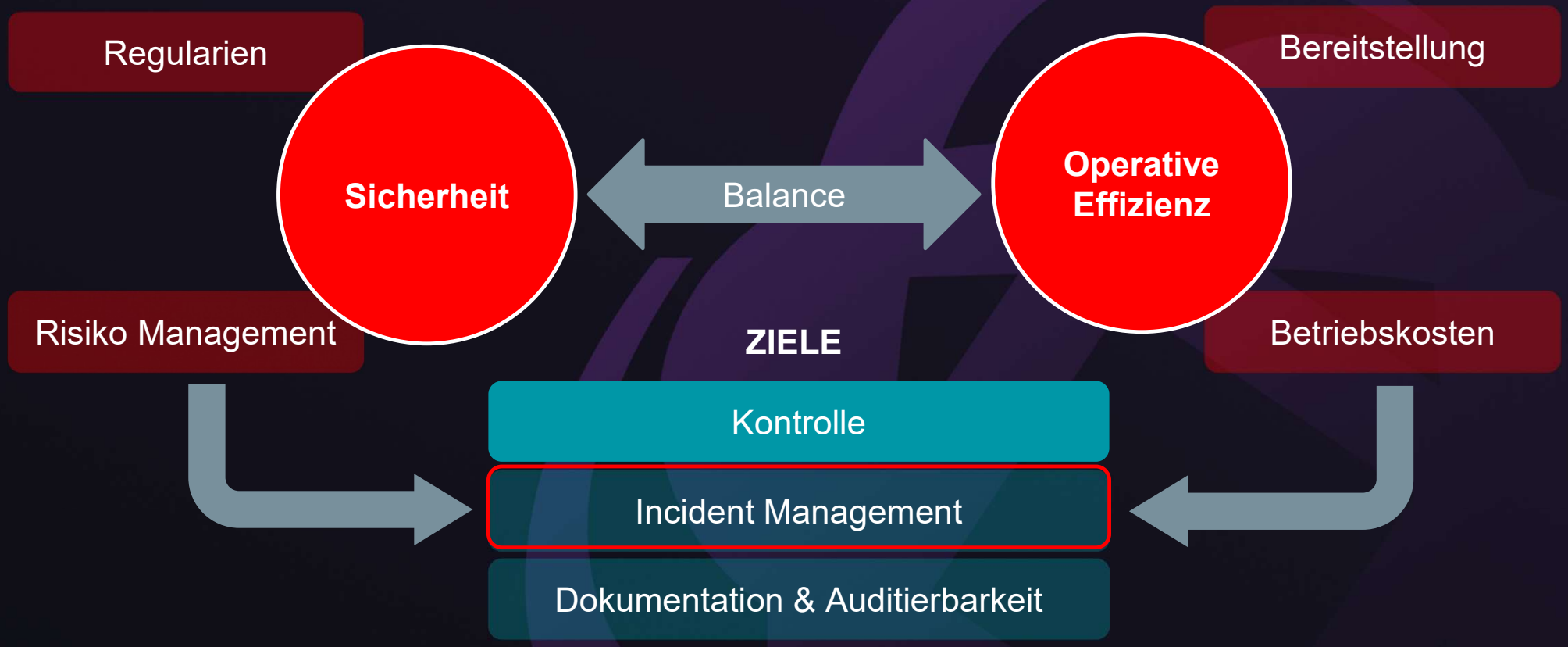
HOHES Risiko

MITTLERES Risiko

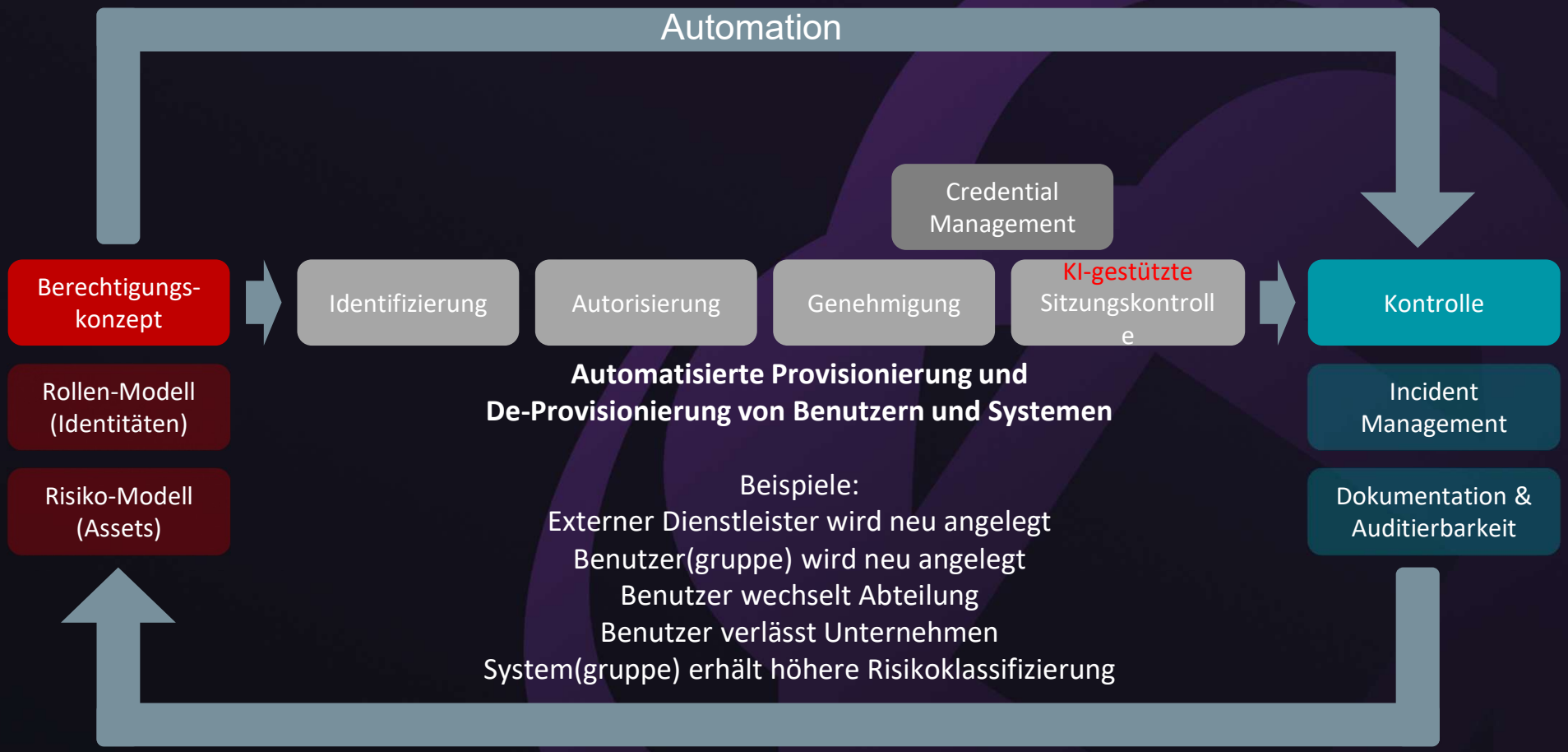
NIEDRIGES Risiko

Business Continuity GEFÄHRDET

Die Herausforderung



Use Case: Automatisiertes Betriebsmodell



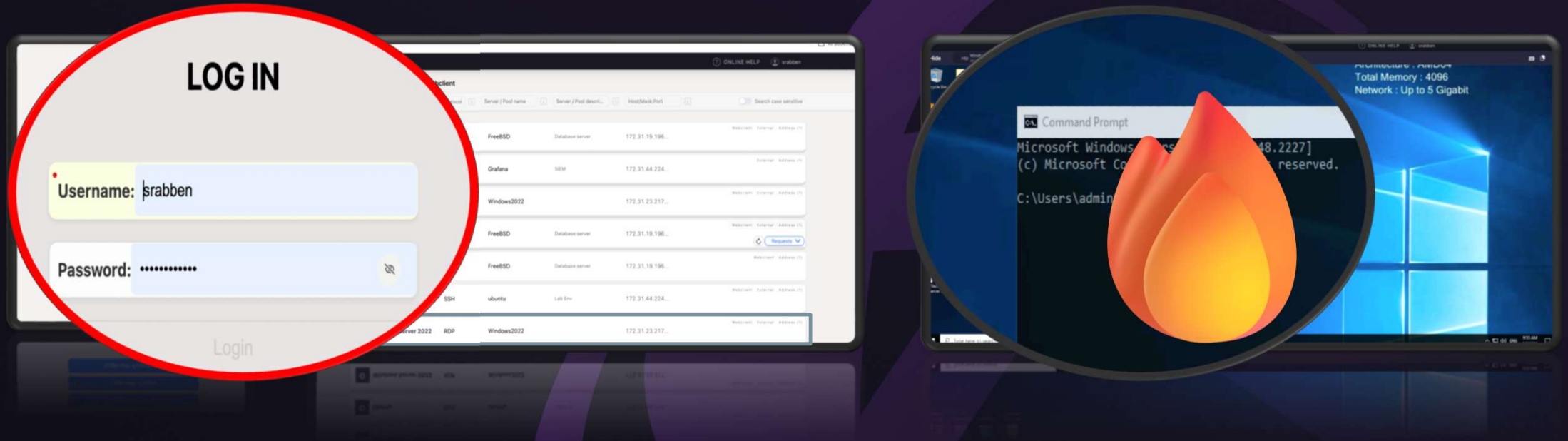
first frame networkers

FUDO SECURITY

KI ZUR MUSTERERKENNUNG
Grundlage zum Incident Management

Die Funktionsweise von PAM

Beispiel: Verbindung zu einem Windows Server (RDP) als Administrator



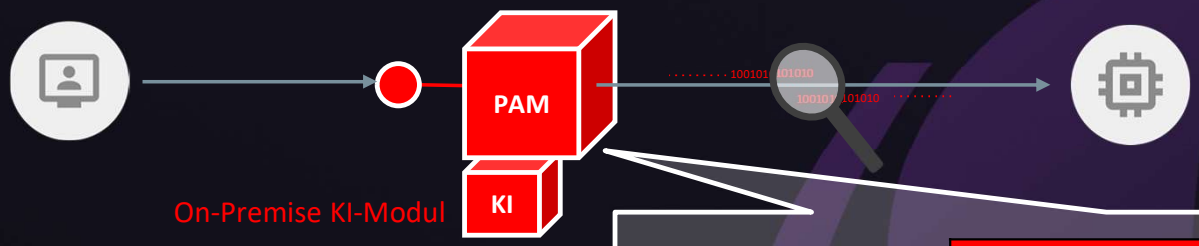
Identitätsdiebstahl?

KI zur Anomalieerkennung

PAM überwacht privilegierte Sitzungen

Benutzerverhalten

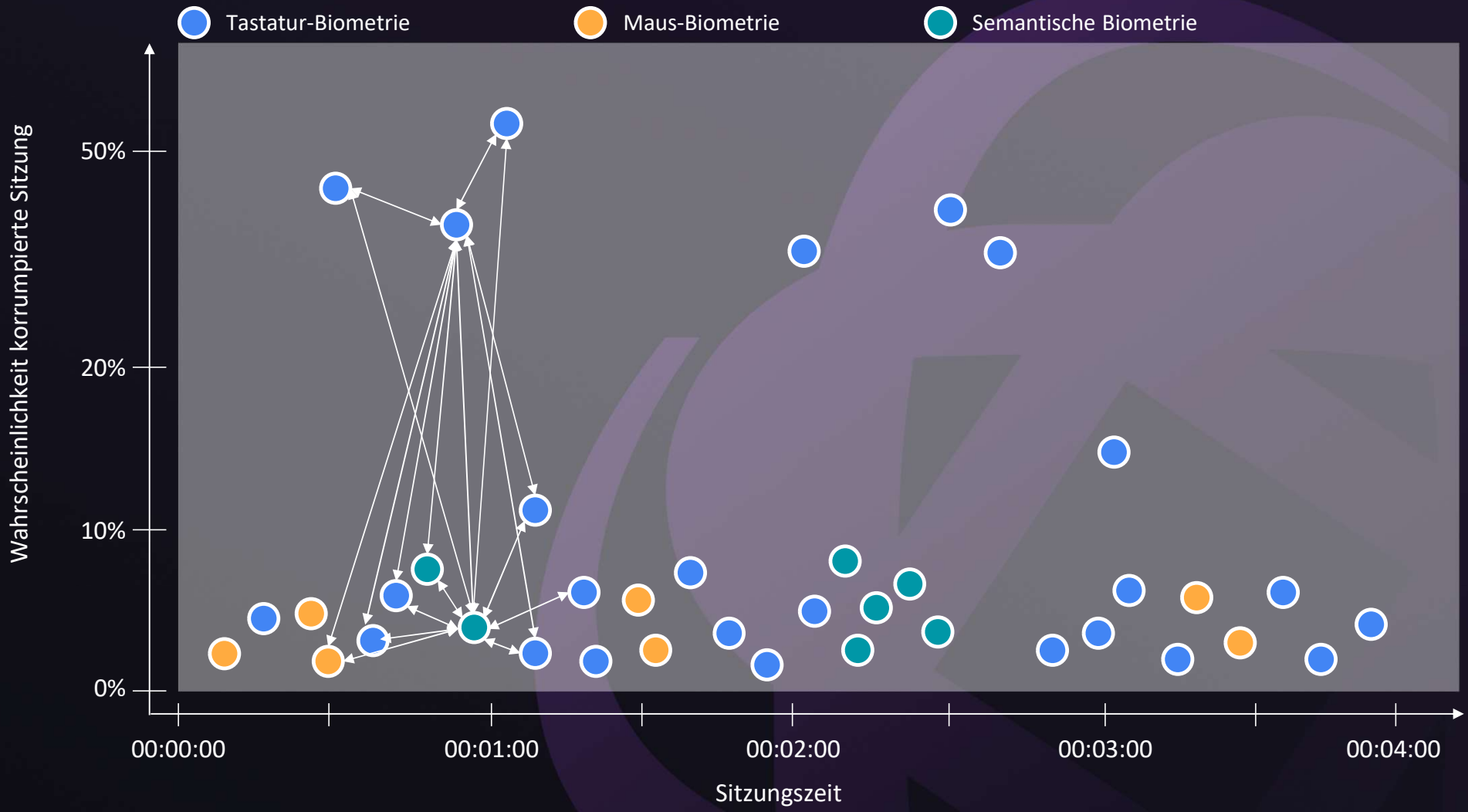
Integriertes KI-Modul analysiert Benutzerverhalten



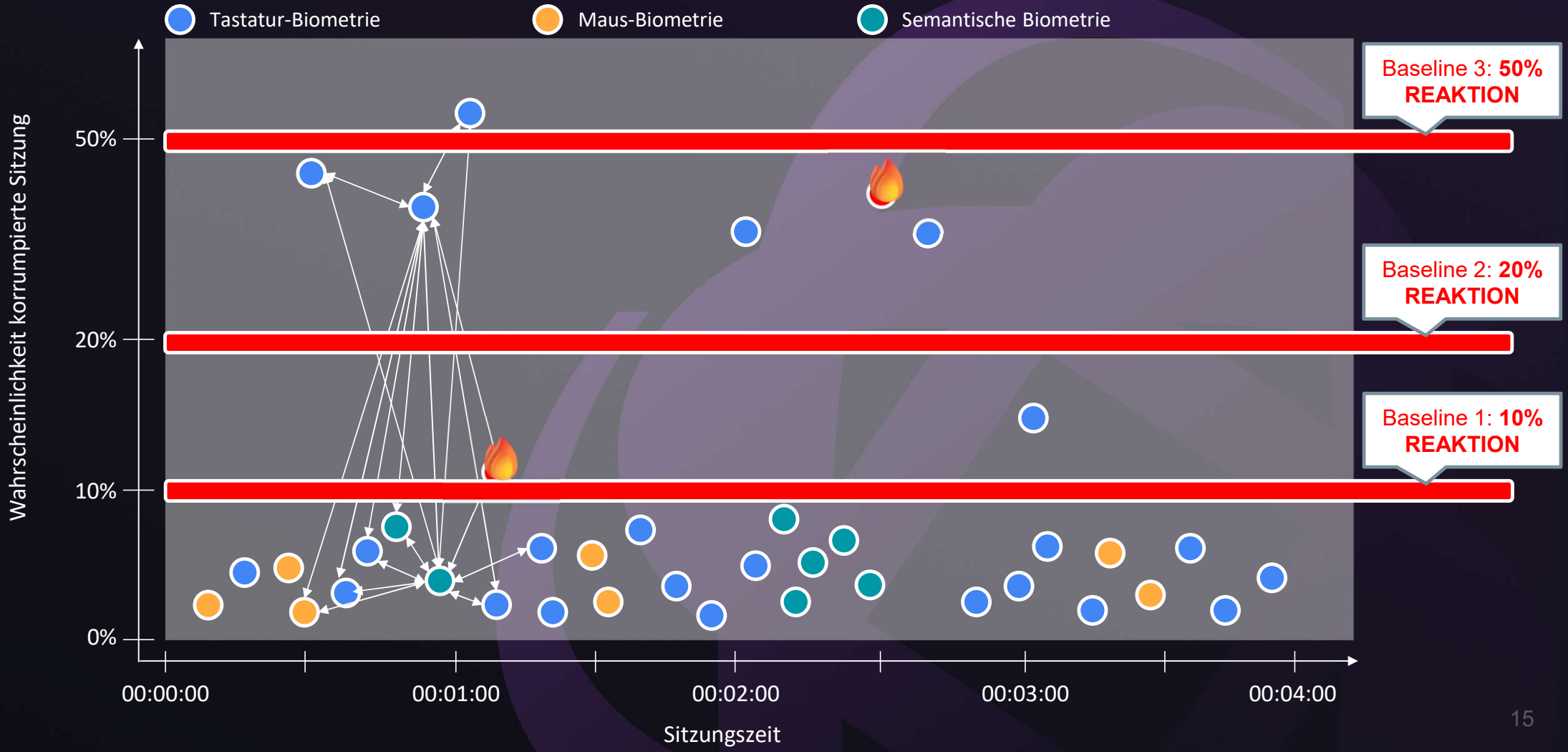
Benutzer-Objekte

Objekteigenschaft: Verhaltensprofil	
Biometrie	Trainingsgrad
Tastatur-Biometrie	75%
Maus-Biometrie	50%
Semantische Biometrie	80%

Analyse durch KI



Analyse durch KI



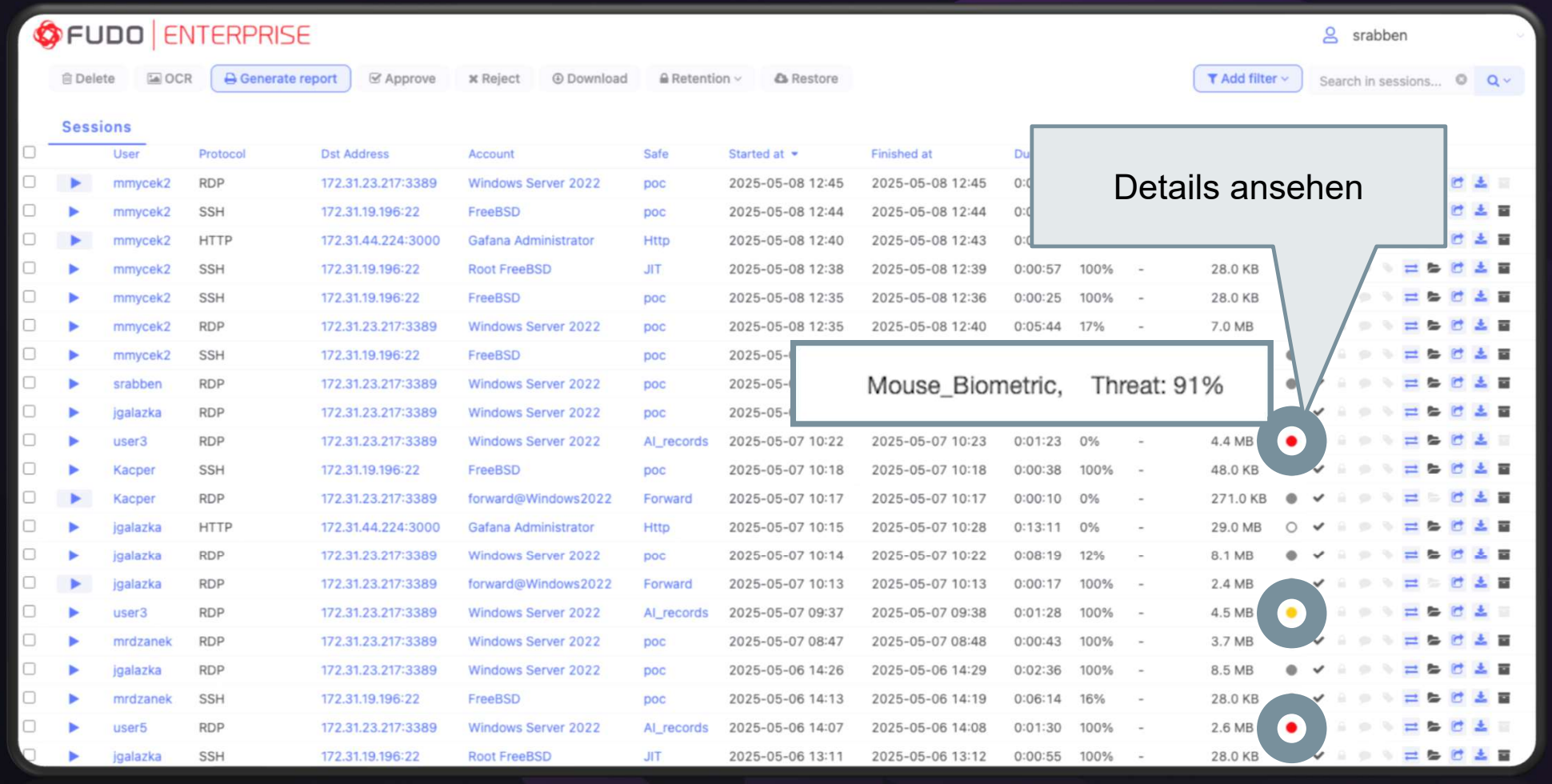
Policy definieren

Verhalten definieren

Messung definieren:
min – max - avg

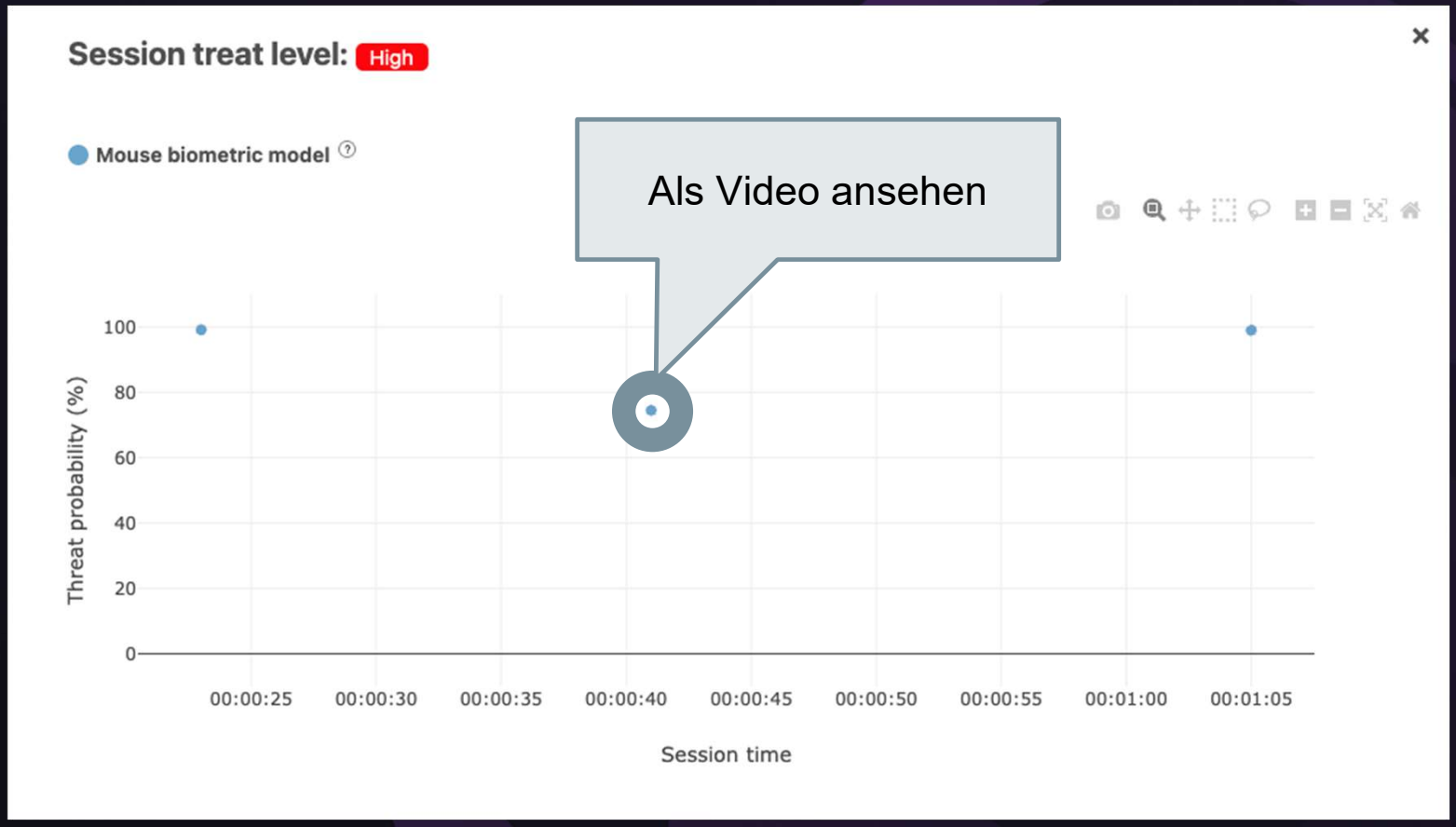
Messwert/Trigger
definieren

Analyse durch KI

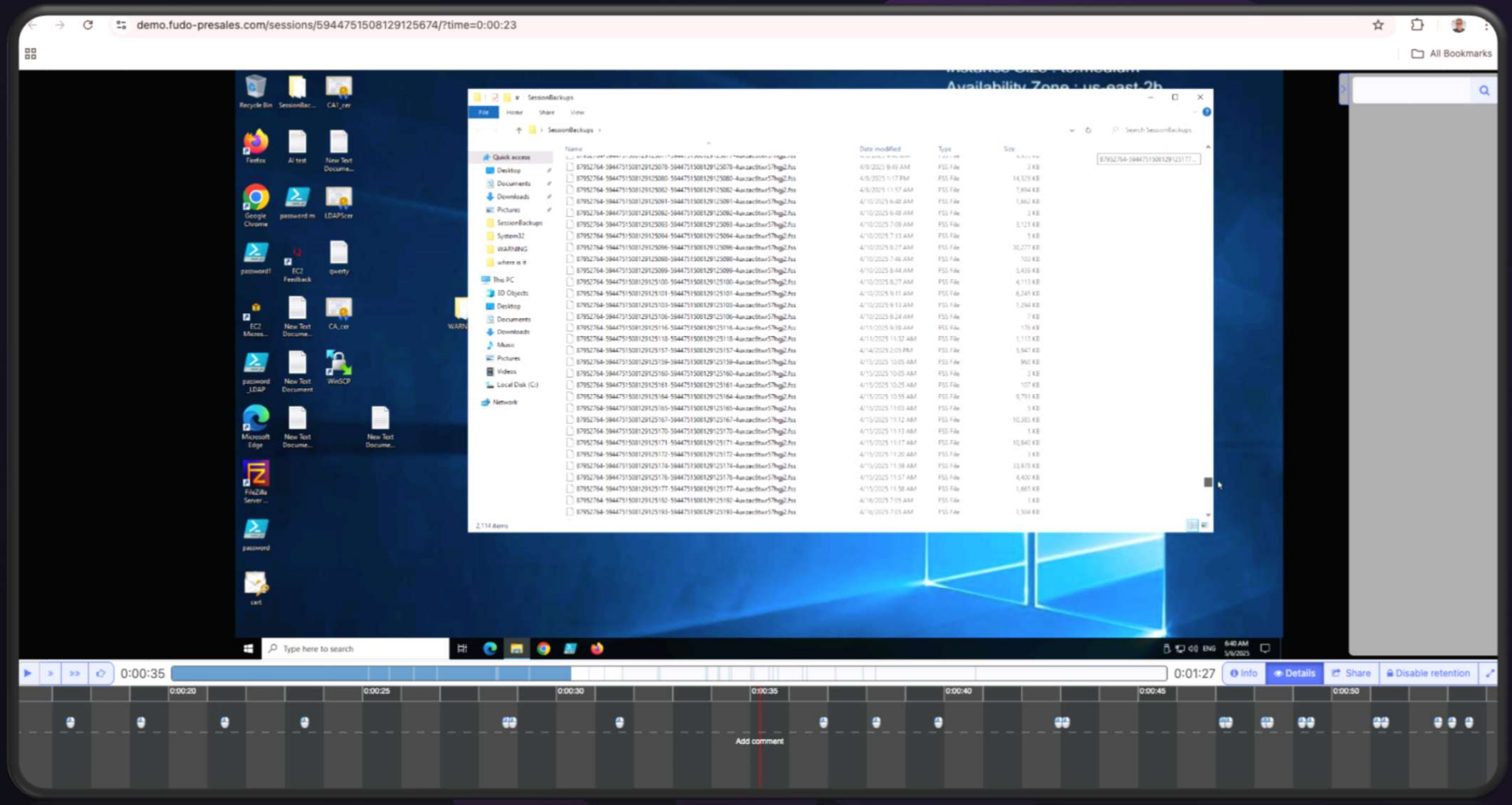


User	Protocol	Dst Address	Account	Safe	Started at	Finished at	Du			
mmycek2	RDP	172.31.23.217:3389	Windows Server 2022	poc	2025-05-08 12:45	2025-05-08 12:45	0:0			
mmycek2	SSH	172.31.19.196:22	FreeBSD	poc	2025-05-08 12:44	2025-05-08 12:44	0:0			
mmycek2	HTTP	172.31.44.224:3000	Gafana Administrator	Http	2025-05-08 12:40	2025-05-08 12:43	0:0			
mmycek2	SSH	172.31.19.196:22	Root FreeBSD	JIT	2025-05-08 12:38	2025-05-08 12:39	0:00:57	100%	-	28.0 KB
mmycek2	SSH	172.31.19.196:22	FreeBSD	poc	2025-05-08 12:35	2025-05-08 12:36	0:00:25	100%	-	28.0 KB
mmycek2	RDP	172.31.23.217:3389	Windows Server 2022	poc	2025-05-08 12:35	2025-05-08 12:40	0:05:44	17%	-	7.0 MB
mmycek2	SSH	172.31.19.196:22	FreeBSD	poc	2025-05-					
srabben	RDP	172.31.23.217:3389	Windows Server 2022	poc	2025-05-					
jgalazka	RDP	172.31.23.217:3389	Windows Server 2022	poc	2025-05-					
user3	RDP	172.31.23.217:3389	Windows Server 2022	AI_records	2025-05-07 10:22	2025-05-07 10:23	0:01:23	0%	-	4.4 MB
Kacper	SSH	172.31.19.196:22	FreeBSD	poc	2025-05-07 10:18	2025-05-07 10:18	0:00:38	100%	-	48.0 KB
Kacper	RDP	172.31.23.217:3389	forward@Windows2022	Forward	2025-05-07 10:17	2025-05-07 10:17	0:00:10	0%	-	271.0 KB
jgalazka	HTTP	172.31.44.224:3000	Gafana Administrator	Http	2025-05-07 10:15	2025-05-07 10:28	0:13:11	0%	-	29.0 MB
jgalazka	RDP	172.31.23.217:3389	Windows Server 2022	poc	2025-05-07 10:14	2025-05-07 10:22	0:08:19	12%	-	8.1 MB
jgalazka	RDP	172.31.23.217:3389	forward@Windows2022	Forward	2025-05-07 10:13	2025-05-07 10:13	0:00:17	100%	-	2.4 MB
user3	RDP	172.31.23.217:3389	Windows Server 2022	AI_records	2025-05-07 09:37	2025-05-07 09:38	0:01:28	100%	-	4.5 MB
mrdzanek	RDP	172.31.23.217:3389	Windows Server 2022	poc	2025-05-07 08:47	2025-05-07 08:48	0:00:43	100%	-	3.7 MB
jgalazka	RDP	172.31.23.217:3389	Windows Server 2022	poc	2025-05-06 14:26	2025-05-06 14:29	0:02:36	100%	-	8.5 MB
mrdzanek	SSH	172.31.19.196:22	FreeBSD	poc	2025-05-06 14:13	2025-05-06 14:19	0:06:14	16%	-	28.0 KB
user5	RDP	172.31.23.217:3389	Windows Server 2022	AI_records	2025-05-06 14:07	2025-05-06 14:08	0:01:30	100%	-	2.6 MB
jgalazka	SSH	172.31.19.196:22	Root FreeBSD	JIT	2025-05-06 13:11	2025-05-06 13:12	0:00:55	100%	-	28.0 KB

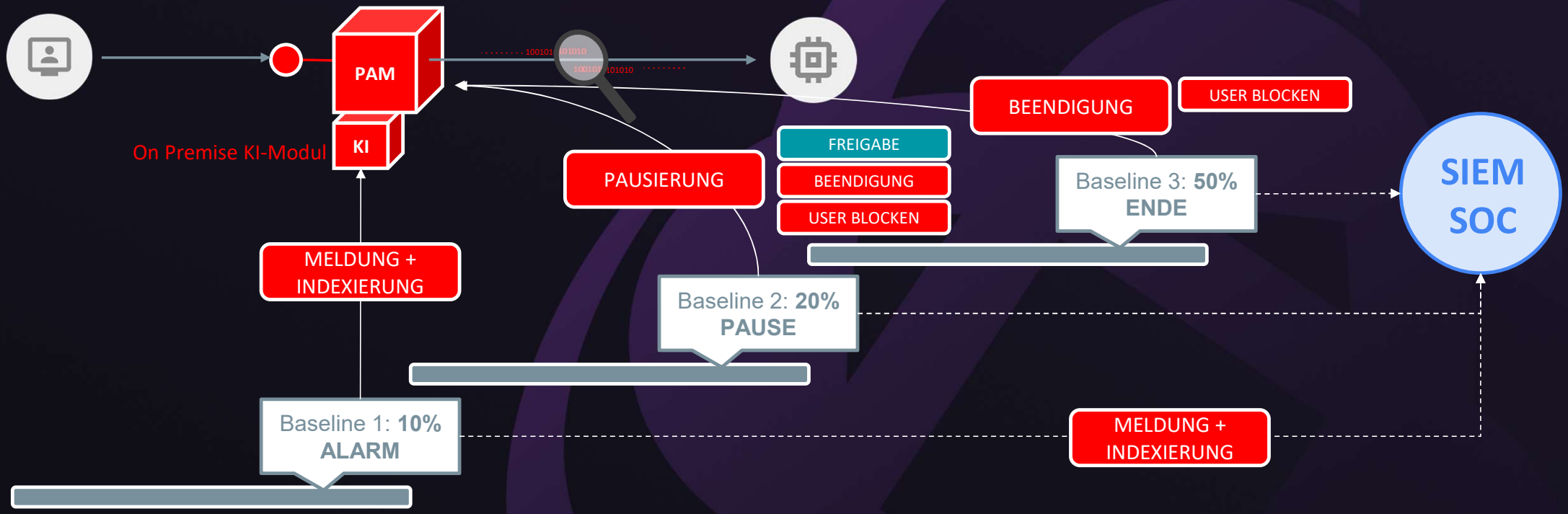
Analyse durch KI



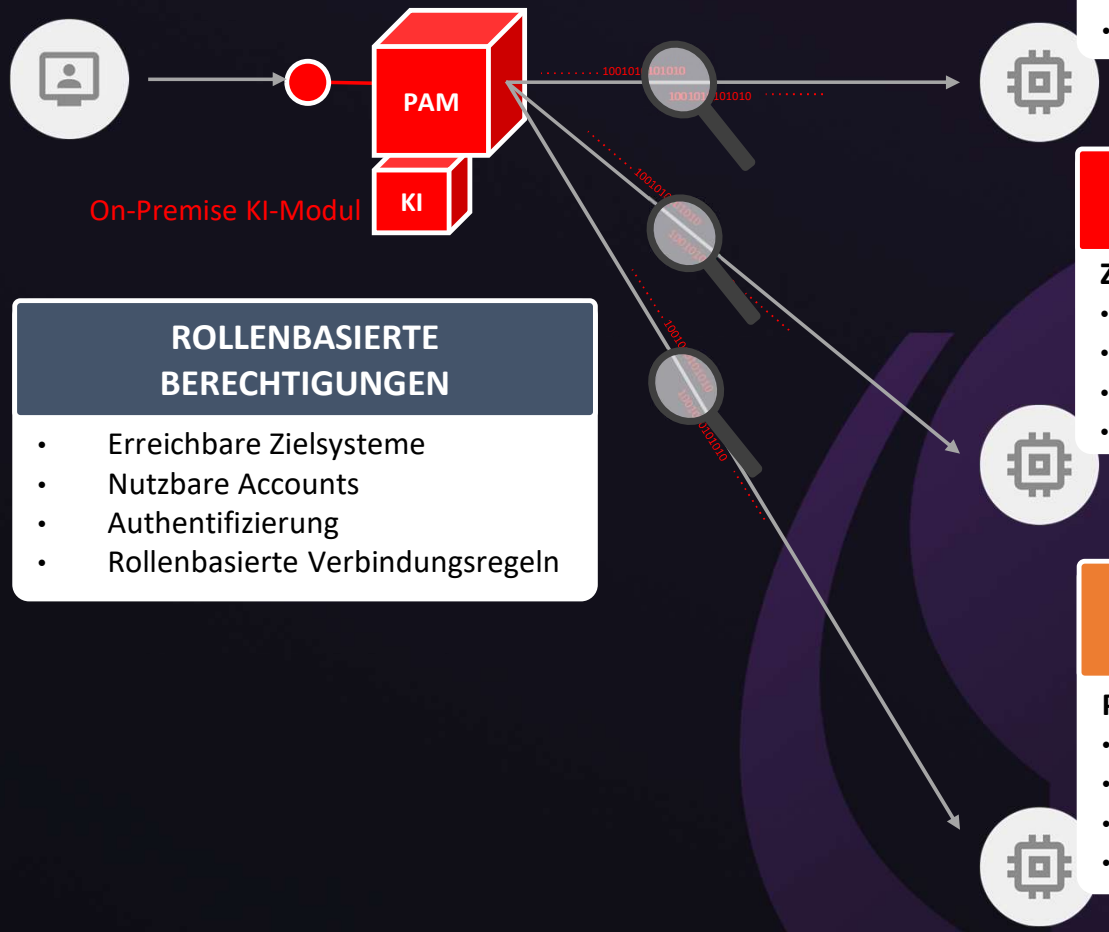
Analyse durch KI



Incident Management durch KI



Best Practises



ROLLENBASIERTE BERECHTIGUNGEN

- Erreichbare Zielsysteme
- Nutzbare Accounts
- Authentifizierung
- Rollenbasierte Verbindungsregeln

RISK 0 SYSTEME
- SEHR HOHES RISIKO -

Zugriff auschließlich über PAM

- Genehmigungsworkflow (4-Augen)
- Multi-Faktor Authentifizierung
- Videoüberwachung
- Passwort-Rotation: alle 120 min

RISK 1 SYSTEME
- HOHES RISIKO -

Zugriff auschließlich über PAM

- Genehmigungsworkflow (2-Augen)
- Multi-Faktor Authentifizierung
- Videoüberwachung
- Passwort-Rotation: wöchentlich

RISK 2 SYSTEME
- MITTLERES RISIKO -

Privilegierter Zugriff über PAM

- Genehmigungsworkflow für Externe
- Multi-Faktor Authentifizierung
- Videoüberwachung für Externe
- Passwort-Rotation: monatlich

GPO Einstellungen

(BSI 200-3)

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.html?nn=128620

Warum Fudo?

GLOBEE AWARDS BRONZE WINNER 2024

Bestes SM

2024 WINNER CYBER SECURITY EXCELLENCE AWARDS

GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2024

NEXT GEN PRIVILEGED ACCESS MANAGEMENT

FUDO SECURITY

24 Stunden

Inbetriebnahme innerhalb von 24 Stunden

Session Management

Bestbewertetes Session Management

Beste KI

Innovation

2024 WINNER CYBER SECURITY EXCELLENCE AWARDS

2024 WINNER CYBER SECURITY EXCELLENCE AWARDS

KI

Bestbewertete KI zur Anomalieerkennung & -abwehr

MADE IN EUROPE

NATO-Sicherheitszertifikat

Sicherheitsarchitektur

Eines der sichersten PAM-Architekturen am Markt
- FreeBSD Unix als gehärtetes Betriebssystem -

SORGENFREIER BETRIEB MIT MANAGED PAM ALS SERVICE

first frame networkers

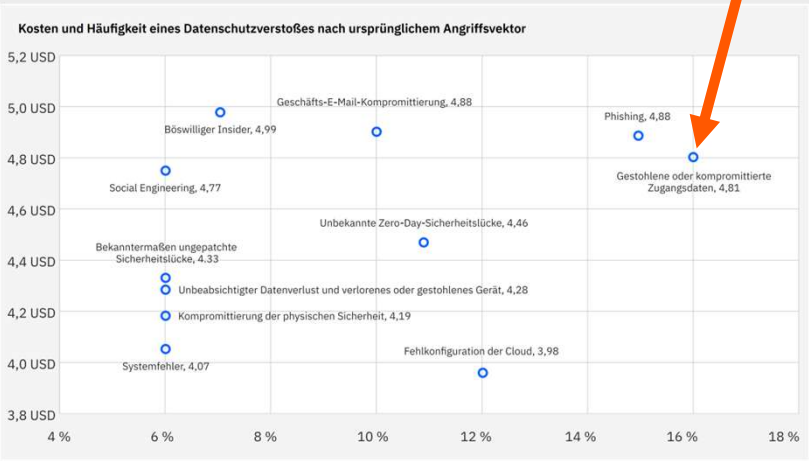
WARUM EINEN MANAGED SERVICE ?

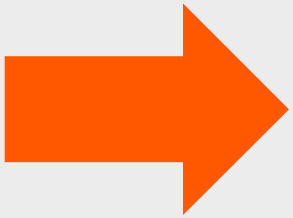
first frame networkers

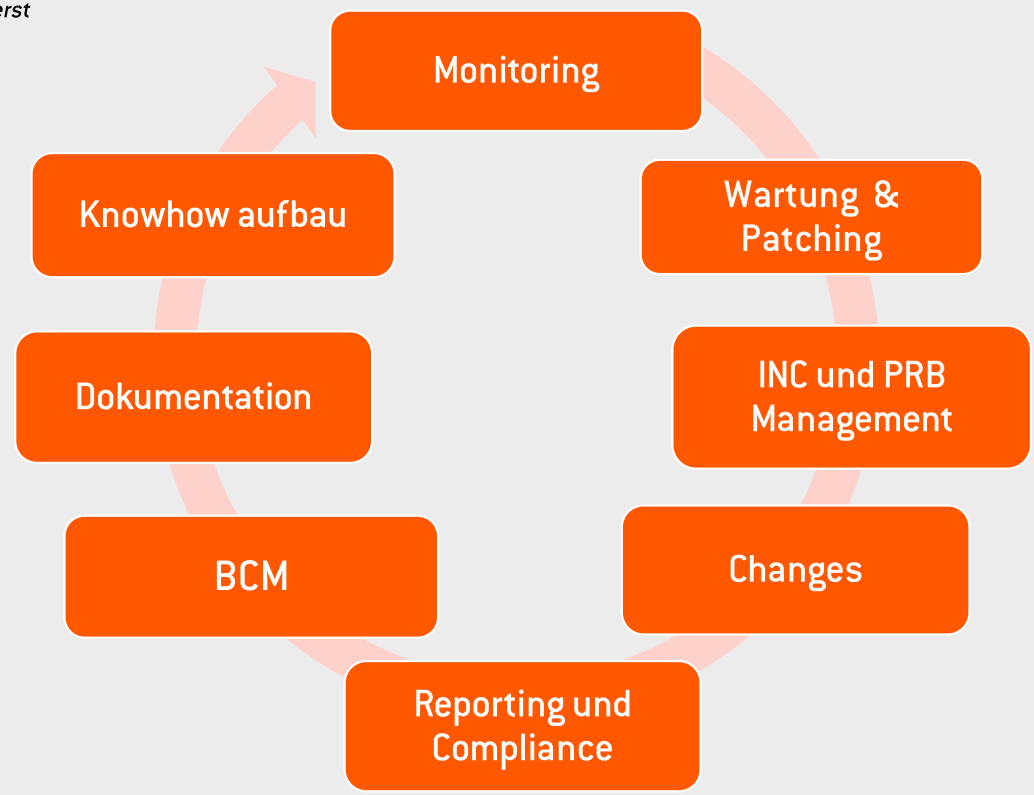
«Angriffe, die auf Anmeldeinformationen basierten, konnten erst nach längerer Zeit identifiziert und eingedämmt werden » [1]

IBM

Cost of a Data Breach Report
2024[1]







[1] - IBM Cost of a Data Breach Report 2024, S.13, Abbildung 7

WIE KÖNNEN WIR HELFEN?

first frame networkers

Betriebsteam:

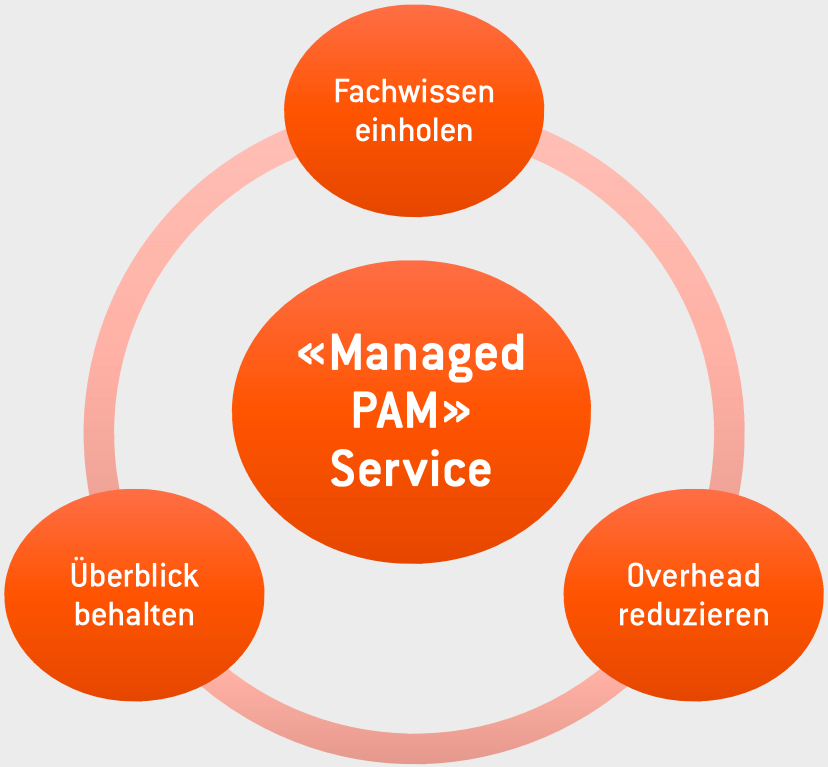
Robin Kiefer

Franz Wachtel

Danilo Giacomini

Martin Schor

Andreas Herger



WAS GENAU?

first frame networkers

Zertifiziertes Knowhow

Regelmässige Wartung & Patching bei CVE's

Schneller 3rd Level Support mit FUDO

24x7 Monitoring mit Reaktion zu Bürozeiten

Regelmässiges Reporting

Issue Management

WIE SIEHT DER WEG AUS?
CALL 2 ACTION

first frame networkers

- Betrieb der PAM Appliance
- Durchführen Projekt
- Evaluieren Entscheid und Offering Projekt
- Proof-of-Concept
- Sessions mit Networker

WEITERE INFOS

first frame networkers

Jetzt unverbindlich einen Online-Termin anfragen.

Wir beraten Sie gerne persönlich.

Managed PAM by first frame networkers

Q & A

first frame networkers

NEXT STEPS

Let's Talk!

- Mit Ihrem Account Manager
- oder mit Danilo Giacomini: danilo.giacomini@firstframe.net oder +41 41 768 08 00

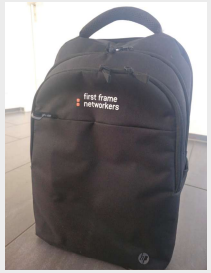
Weitere Infos

- Managed PAM Services – first frame networkers ag
- Factsheet FUDO Security PAM
- Blogartikel - Sicherer Umgang mit Privileged Access: Warum Unternehmen auf PAM-Lösungen setzen sollten

FEEDBACK-FORMULAR

first frame networkers

- Herzlichen Dank für Ihre Teilnahme am heutigen Webinar.
- Ihre Meinung ist uns wichtig.
- Daher bitten wir Sie um eine Minute Ihrer wertvollen Zeit für die Feedbackumfrage.
- Unter allen ausgefüllten Fragebögen verlosen wir drei FFN-Rucksäcke.



- Den Link finden Sie auch im Chat: https://forms.office.com/e/bcrNsemj3t

Herzlichen Dank

first frame networkers